

# Safe and secure:

## Top 10 threats to network security

1 It is vital to enforce adherence to security policies, ensuring that users maintain the integrity of systems through such things as the ownership of files and simple passwords etc. Without automation of security auditing, it is easy for careless shortcuts to open security holes on systems, for example, companies should ask how many users don't have passwords on shared directories for their desktops.

2 The complexity of e-business systems can be daunting and there are ever more access points on the network for IT managers to monitor. The insistence on trying to manage all this in-house can hamper security efforts. A little bit of knowledge can be a dangerous thing and it is best to get in a specialist provider whose core business it is to keep up to date with new developments and to apply the best combination to your business, so you can in turn concentrate on your core business and not IT issues.

3 The practice of extending the network for use by suppliers, customers and partners increases the number of people with access to your network and therefore proportionately increases the risk of attack. The issues arising from this are two-pronged: any breach to your system could affect their business as well as your own and in this way could negatively affect your external relationships; in turn, any insecure points in their network can become your problem when the systems are connected – you might unwittingly be exposing your business to increased points of entry on the overall network.

4 A lack of understanding of specific potential threats can negate investment in security. It doesn't matter how much money is spent on securing a system if there is not a complete understanding of all the threats to electronic assets.

5 An inability to understand the importance of system security by boardroom-level executives means security is not made a financial priority. A lack of appreciation of the potential implications of breaches means sufficient funds are not budgeted for. Executives at the highest level must be made to understand that, in an e-commerce-focused environment, no system equals no business.

6 There is a pervasive refusal to recognise that because systems evolve, security must evolve with them. Security is not something that can simply be installed once and forgotten. There is a requirement for ongoing monitoring, maintenance and upgrading as the system is similarly altered or improved. All components of a system, including servers, routers, terminals, access points, wiring, even physical factors such as temperature and power sources, should be examined as a matter of course.

7 A lack of understanding of the kinds of tools available and what they do means that many security solutions are not as effective as they could be. Many firewalls only keep out amateurs and most companies will need a higher level of protection than they currently possess. But they may not know about the tools they can use to obtain greater security.

8 The historical fire fighting approach will limit security efficiency. A proactive, rather than reactive approach, actively monitors applications, as well as network and systems infrastructure, to alert you to system weaknesses BEFORE they become a problem.

9 Internal hackers can represent as big a threat as external hackers and virus-perpetuators. While external intruders are the obvious threat, nobody knows the inherent weaknesses of a system better than the employees who work with it every day and internal mischief-makers can use their passwords to access sensitive data, whether their intent is malicious or otherwise. A comprehensive set of layered defences could require the inclusion of physical measures such as restricted areas or card keys, on top of firewalls, virus- and intruder-detection software and the like.

10 Denial of service attack is a preferred method of destruction for your advanced hacker. This is an attempt to prevent legitimate users of a service from accessing those functions in a system, by flooding a network to block traffic or disrupting connections. Resources used illegally or wrongly can also cause denial of service, such as storing data or software on your system, taking up disk space. A complete security solution will separate critical functions from non-critical activity and establish a base of standard activity against which to measure extraordinary activity, with diagnostic tripwire type tools to detect changes in configurations.

By Steve Bird

Director and Senior Solutions Architect

Kinetica

About Kinetica

Kinetica, formerly known as Full Spectrum, is the market leader in designing, implementing and maintaining Enterprise Management Systems which

empower businesses to reap the benefits of their IT infrastructure. The company delivers management systems that are focused on supporting business processes and delivering complete control and visibility of the diverse and disparate elements of clients' IT infrastructures. Kinetica delivers the full spectrum of EMS solutions from industry leading vendors to tailor a professional, complete and reliable solution, using products that expertly match business needs. Visit the Kinetica web site at: [www.kinetica.com.au](http://www.kinetica.com.au) for more details.